REMARKS

Applicants' respond hereby to the final Office Action mailed September 7, 2007, in the above-identified application. Claims 1-23 remain pending hereafter, where claims 1 and 10 are the independent claims.

In the final Office Action, the rejection of Claims 1-19 and 22 (that is, all of pending claims 1-23) under 35 USC §102(e) as anticipated by US Patent No. 5,414,844 to Wang is maintained (on final). With respect to independent Claims 1 and 10, the Examiner states that Wang discloses a method and apparatus for controlling access to an object in a data processing system, including receiving an access request to access the object from a task (col. 5, lines 60-63); classifying the access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task (col. 5, line 66 through col. 6, line 8); granting the task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class (col. 6, lines 8-1); and, in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data (col. 6, lines 12-23).

In the "Response to Arguments," at paragraphs 3-7 of the final Office Action, the Examiner explains the reasons that applicants' arguments were deemed not to have overcome the rejection of claims 1-23 in view of Wang under Section 102(e). The Examiner refers as well to applicants' arguments for patentability of independent claims 1 and 10, stating that Wang, contrary to applicants' assertion in their June 11, 2007, Amendment, discloses the step of classifying an access request an object from a task, the step including "classifying the access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task" (col. 6, lines 8-11).

Applicants understand that Wang discloses classifying objects into classes by use of his data control object 40. The data control object file 40 comprises a library object 42, and Access Control Model Object (ACMO) 44. ACMO 44 includes an owner identity 46 with the name of the user owning the library object. An explicit authorization parameter 48 is also included, utilized to identify identities of specific individual users, and the authority level (or role) the user has with respect to the library object 42. The ACMO44 also includes a shared authorization parameter 50 that controls a list of identities of multiple users and their respective authority level or roles with regard to access to the plurality of library objects that use the shared parameter.

Applicants find that Wang does not disclose their claimed step of classifying. Applicants' step of classifying sets forth: classifying the access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task. As mentioned, Wang utilizes a method by which public access to a large group of data objects is centrally controlled by use of data object 40 to classify access to one of two classes in association with the user, or user's role for access. Some users can read an object, and some users can write to an object. Nowhere does Wang disclose managing the access control where the stored access control data is based not just on a users role to access either non-critical or critical objects, but on the task requesting access.

At page 12 of applicants' specification, lines 1-19, applicants describe the inventive operation with reference to Fig. 4. That is, on receipt of a request to access an object 250 from a task 270, at block 301 of Fig. 4, access controller 280 classifies, at block 302, the request into one of a critical and non-critical task in dependence on stored access control data 285, associated with the object and task. Access to a critically classed object is granted or denied

in dependence on the content of access log 290 and the stored access control data 285.

Wang's Specification at col. 5, line 66, through col. 6, line 11, describes the access. "After access of a particular document has been requested, as determined in block 82, block 84 illustrates a determination of whether or not the user requesting access is a listed user. By "listed user" what is meant is a user whose identity is specifically set forth within ACMO for the document in question. If the user requesting access to the document is a listed user, as determined in block 84, block 86 illustrates a determination of whether or not the user in question possesses a sufficient authority level for the action desired. If not, an error message is returned, as illustrated in block 88. If the user in question has sufficient authority level for the action desired, then access is granted, as depicted in block 90."

While the Examiner asserts that Wang discloses granting the task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class, at col. 6, lines 8-11, applicants' again respectfully disagree. Wang's col. 6, lines 8-11, states that if a user in question does not have sufficient authority to access a requested document or object, access to the document is denied, and if the user has sufficient authority, access is granted. Wang does not grant task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class. Wang may grant access in some sense, but does not store data indicative of the access in an access log, a requirement of the independent claims.

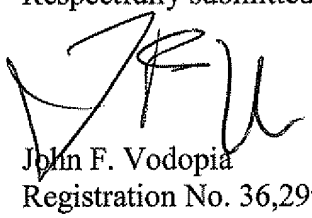
And while the Examiner asserts that Wang teaches that in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data (col. 6, lines 12-23), applicants again respectfully disagree. The cited Wang text merely states that, with respect to

block 84, if a user attempting to access is not a user specifically set forth in a ACMO for the document in question, block 94 determines whether a public authority parameter includes a reference to a shared authority parameter. If there is no detected reference to a shared authority parameter an error is returned and access denied, and if so, access is limited by the shared authorization parameter. Wang does not teach or suggest that in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data at col. 6, lines 12-23. While a Wang user must meet the requirements for determining authority level for accessing an object classified in a critical class to gain access using a shared authorization parameter, Wang's disclosed structure and operation is not equivalent to granting or denying access to the object by the task in dependence on contents of applicants' claimed access log, and applicants' stored access control data.

Applicants, therefore, respectfully assert that independent claims 1 and 10 are not anticipated by Wang for at least the reasons set forth, and request withdrawal of the rejections of claims 1 and 10 under Section 102(e) in view of Wang. Claims 2-9 and 20-22 depend from claim 1, and are patentable therewith. Likewise, claims 11-19 and 23 depend from claim 10, and are patentable therewith. Applicants' further request withdrawal of the rejections of claims 2-9 and 11-23 under Section 102(e) in view of Wang.

If the Examiner believes that a telephone conference with applicants' attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,



John F. Vodopia
Registration No. 36,299
Attorney for Applicants

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343

JFV: tb